THE RIGHT TO PRIVACY

BY RUPERT GRANVILLE GLOVER, M.A.(HONS), LL.B.(HONS),
Lecturer in Law, University of Canterbury

> "[E]lectronic surveillance is a powerful technique. It may be used for good and evil ends. More importantly, it raises in a critical way the moral dilemma faced in all democratic societies of justifying illiberal means, which strike at the hearts of individual liberty, by reference to ends sought to be achieved. This is because the whole purpose of electronic surveillance of suspected criminal activities is to obtain information surreptitiously at a time and place where the suspect believes he is free to speak without being overheard. The use of a listening device planted in private property can only be regarded as an intrusion into the privacy of the home. . .".
>
> "It would be intolerable in a free society if the agencies of the state, or for that matter, private individuals and organisations, were free to monitor private conversations at will and make whatever use they chose of material obtained as a result. However, few would dispute that in very special circumstances the natural of potential offending and its clear danger to the fabric of society may justify the use by the state of electronic surveillance. It is a matter then of striking a balance between the various public and private interests involved." Richardson J in his dissenting judgment to *R* v *Menzies*, Court of Appeal.
>
> [1982] 1 NZLR 40, 51-2

Advances in technology have led to a startling increase in the possibilities available to those who wish to obtain private information about others, either for legitimate or illegitimate purposes. Invasions of the individual's private life can be separated into three broad groups:

1. *The collection of information by direct surveillance*: the sophistication of electronic and optical surveillance devices advances by the day. It is now very difficult for an individual to know whether or not his private life is being monitored by such a device, since miniaturisation has made physical detection difficult. The logical response — electronic detectors — involves too much expense and complexity to be of practical assistance to the average person. Mail and telephonic communications are, of course, highly vulnerable.

2. *The collation of information by data processing*:[1] the advent of the micro-chip and the development of ever more sophisticated and efficient computers has made it possible to store and recall vast amounts of private information about individuals. From a person's bank statements, credit card transactions, hire purchase records, education records, criminal and traffic records, insurance policies, club membership, visa and passport applications and travel movements, employment records, medical history etc., it is possible to build up a composite and detailed picture of an individual's life with a speed and thoroughness that was hitherto impossible.

[1] See appendices E and H of "Privacy and the Law", a report by the Committee on Privacy of *Justice* (the British Section of the International Commission of Jurists) 1970.

3. *Publication and dissemination of private information by the mass media*: in bygone days gossip and scandal, although of some annoyance to their subjects, were of necessarily limited scope. Today, with mass audiences for the electronic and print media numbering millions, it is possible for a piece of information which is distressing to some private person to be flashed to the eyes and ears of the vast numbers of people world-wide.

It is instructive to consider the following examples of invasions of privacy:[2]

1 You have a secluded garden, overlooked only by a hill two miles away. One day you are kissing your wife in the garden when a stranger, standing on a highway on the hill, takes a photograph of you through a powerful telephoto lens.[2a]

2 You and your co-director are in your office, discussing your company's future marketing strategy. From premises across the street your trade rival, with the permission of the occupier, monitors your conversation with a laser beam device.

3 A national credit information bureau makes every reasonable effort to get its information only from the most reliable sources. The agent whom they employ in your locality has a grudge against you and knows about some past skeletons in your cupboard, an accurate version of which he includes in a report on you which goes on their file. Your credit is ruined.

4 Your employer, unknown to you, has your wife followed and her friends and neighbours interviewed. The results, with adverse (but true) comments, go down on your personnel record.

5 You are a respected member of your local community, but not in any sense a public figure. One day, your local newspaper publishes an article about you in which they allude to the facts that:

(a) twenty-five years ago you were convicted of stealing;

(b) ten years ago, you had an affair with a married woman; and,

(c) your mother died in a lunatic asylum.

All these statements are true.

6 Your only child, a successful actress, is killed in a car crash. Reporters telephone you night and day, and your house is besieged by photographers from the Press and the television companies, who take pictures of you and your wife whenever you show yourselves at the door. These are published in the national Press and on the television news bulletins.

---

[2] Based on appendix C of the above-mentioned report.

[2a] If the stranger is a private investigator he must have your written consent under s.52 of the Privator Investigators and Security Guards Act 1974.

7 You are under contract as the Managing Director of a company. You are a homosexual, but have fought this with almost complete success. Very few people know about this, but one of them happens to be a close friend of the Chairman of the Board, whom he tells in strict confidence. The Board exercises its contractual option to terminate your contract and you are given no reasons.

In none of these cases would there be any redress as New Zealand's law now stands, nor would anyone have committed any criminal offence.

What then, is the current state of the law protecting privacy? Does the law protect privacy adequately or even at all? Can an individual defend himself or herself against invasions of his or her private life? It is the purpose of this paper to provide answers to some of these questions.

The right to privacy is recognised as a fundamental human right in Article 12 of the United Nations Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.[3] The 1967 Stockholm Conference of the International Commission of Jurists was convened specifically to discuss the right to privacy. It included, *inter alia*:

> "(1) The right to privacy, being of paramount importance to human happiness, should be recognised as a fundamental right of mankind. It protects the individual against public authorities, the public in general and other individuals. . .".

The Conference recommended:

> "(14) . . .that all countries take appropriate measures to protect by legislation or by other means the right to privacy in all its different aspects and to prescribe the civil remedies and criminal sanctions required for its protection."

The problem involved in any consideration of privacy is to balance the individual's needs against the legitimate interests of the community. Accordingly there will always be a variety of opinions about the exact content and scope of privacy, and it is probably as well not to attempt exhaustive definitions. Generally, however, it is probably reasonable to see privacy as "that area of a man's life which, in any given circumstances, a reasonable man with an understanding of the legitimate needs of the community would think it wrong to invade".[4]

Thus privacy requires protection by the law only in as much as, without such protection, it would be infringed without just cause by others. Obviously the risk of such infringement is related to factors such as population density, the degree of organisation of the social structure and the technological level of the society in question. At the same time, freedom of expression and the free flow of knowledge ought to be preserved, and society must also have available to it enough personal information for proper administration. Freedom of the press must also be preserved in a democracy, but there is a fundamental difference between truths which the

---

[3] Which came into force in New Zealand on 28 March 1979.

[4] Justice Report, op.cit. para. 19.

public has a right to know in its own interest and "those which merely gratify voyeuristic curiosity at the expense of another's suffering or embarrassment".[5] The law should be able to protect privacy in a way which would not have an adverse effect upon the freedom of the press.

New Zealand law does not at present recognise any general right to privacy, and there was none at common law. Thus any protection which is provided is coincidental. The obvious area in which any such protection might be expected to occur is in the law of torts. There appears to be no reported decision which determines conclusively whether a tort of invasion of privacy exists, although a majority of the High Court of Australia have rejected the idea.[6] Sometimes, however, it may be possible to bring invasion of privacy within another tort. For example, a trespass may have taken place and the Court will take all the injury to the plaintiff into account in assessing damages.

But trespass is a limited remedy because the interference with the plaintiff's interest must be direct: usually physical contact with the plaintiff or his or her property will be required. In addition, where it is a question of trespass to land or chattels, an action will only lie if the plaintiff is entitled to possession of the land or chattels involved. So an owner-occupier or a tenant could sue, but a lodger, hotel guest or hospital patient could not. As well, there will be no civil remedy for optical surveillance from outside the plaintiff's property, or for the use of listening devices where no physical entry is involved.[6a] There will also be no remedy if the person having possession of the property is a party. Trespass to chattels will lie where there is an unauthorised search or inspection of confidential documents legally in the plaintiff's possession, but if the documents are lawfully in the possession of a third party at the time when the inspection takes place, the plaintiff will have no cause of action.

Shadowing or following a person will not give rise by itself to an action in trespass. But in one New Zealand case[7] it was held that a charge of behaving in a disorderly manner may be appropriate if the defendant's "conduct or behaviour is such that it constitutes an attack upon public values that ought to be preserved".[8] In this case a man was so charged for following, without otherwise molesting, a young woman on a street at night.

The tort of nuisance is committed where there is an unreasonable interference with the use or enjoyment of land resulting in damage. This may cover some invasions of privacy, but the plaintiff must usually have an interest in the land,[9] and it is doubtful whether nuisance would extend to watching from outside land.[10]

---

[5] Ibid., para. 27.

[6] *Victoria Park Racing and Recreation Co* v *Taylor* (1937) 58 CLR 479.

[6a] But there may be a criminal remedy under the Crimes Amendment Act 1979. As well, private investigators may not undertake optical surveillance without the written consent of the subject: see footnote 2a above.

[7] *Police* v *Christie* [1962] NZLR 1109.

[8] Ibid per Henry J at 1113.

[9] *Malone* v *Laskey* [1907] 2 KB 141.

[10] *Lyons* v *Wilkins* [1899] 1 Ch. 255.

Without going into the complexities of the law of defamation, it can be said that although it affords some protection of privacy it is unlikely to prevent invasions in several areas. Where there is unnecessary and unreasonable disclosure of embarrassing private facts about the plaintiff, it will nevertheless be a complete defence if the facts are true, although the onus is on the defendant to prove their truth. However, in the context of criminal libel,[11] the plea of justification is more complex and includes both truth (or reasonable belief of truth) and public benefit.[12]

The unauthorised use of a person's name, identity or likeness may sometimes lead to a successful defamation action. In one case[13] an amateur golfer succeeded on the basis that there was an innuendo that he had compromised his amateur status by being depicted with brand-name chocolate protruding from his pocket. If he had been a professional the invasion of his privacy would have been the same, but he would have had no remedy.

There is also no remedy for the defamation of the dead, whether the information published is true or false, no matter how much distress is caused to the living as a result.

Copyright may afford protection of privacy, but depends on the copyright being vested in the plaintiff. An English court held the distressful publication of photographs of a murder victim to be a breach of copyright justifying exemplary damages,[14] but such cases will be unusual.

Contractual relationships may protect privacy where there are express or implied terms in the contract, and this is particularly so with contracts of employment. However there is usually no protection for employees against disclosure by their employer of their performance in lie-detector or personality tests.

Breach of confidence obviously involves issues of privacy and falls into three main categories. The first is abuse of private confidence. In an old case[15] the plaintiff obtained an injunction to prevent the defendant from disclosing confidential private material contained in letters (which had been returned to the plaintiff but of which the defendant had kept copies) written by the plaintiff to the defendant. It was held that the plaintiff had a right of property to the letters. This case has been used extensively by American Courts in privacy cases.[16]

The second category is abuse of commercial confidence. Lord Greene MR said ". . .the obligation to respect confidence is not limited to cases where the parties are in contractual relationship. . .If a defendant is proved to have used confidential information, directly or indirectly obtained from the plaintiff, without the consent, express or implied, of the plaintiff, he will be guilty of an infringement of the plaintiff's rights".[17]

---

[11] See Crimes Act 1961, s.211.

[12] See Crimes Act 1967, s.214.

[13] *Tolley* v *Fry* [1931] AC 333.

[14] *Williams* v *Settle* [1960] 2 All ER 806.

[15] *Gee* v *Pritchard* (1818) 2 Swan 402.

[16] See Warren and Brandeis [1890] 4 Harv. LR 193, 204fn.

[17] *Saltman Engineering Co.* v *Campbell Engineering Co.* (1948) [1963] 3 All ER 413n at 414. This was subsequently applied in *Peter Pan* v *Corsets Ltd.* [1963] 3 All ER 402 and *Seager* v *Copydex* [1967] 2 All ER 415.

The third category is abuse of marital confidence. In a well-known case a wife succeeded in a claim that the marriage relationship itself imposed an obligation of confidence on both parties and that the Court had jurisdiction to restrain her husband from publishing the intimate details of her married life.[18] In the same case it was held that the Court can exercise its equitable jurisdiction in such matters independently of any right at law. In a subsequent case Megarry J proposed a general test: ". . .if the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence, then this should suffice to impose upon him the equitable obligation of confidence".[19]

Negligence may sometimes be relevant to privacy, even though most infringements concern intentional conduct. In one New Zealand case a doctor was held liable to a woman who suffered nervous shock as a result of his giving an accurate certificate of her condition to her estranged husband.[20]

Until recently it did not seem that the tort of negligent misstatement was sufficiently developed to protect a person about whom erroneous non-defamatory information is given. That is, if A said something to B about C's private life which resulted in B's refusing to employ C, C would have been without remedy. But two recent English cases cast doubt on this. In the first,[21] the UK Ministry of Housing was entitled to repayment of compensation it had paid in a town and country planning matter. This right was lost, however, owing to the negligence of a council employee who issued a conclusive ceritficate that the land in question was free of charges. The English Court of Appeal held that the Council employee, and vicariously the Council, was liable to the Ministry. Salmon LJ pointed out that this created a new category of negligence, since the Ministry was not misled by any careless statement made to it by the defendants or made by the defendants to someone else who the defendants knew would be likely to pass it on to a third party, such as the Ministry, in circumstances in which the third party might reasonably be expected to rely upon it.

In the second case,[22] solicitors negligently failed to warn a testator that attestation of his will by a beneficiary's spouse would invalidate the gift to that beneficiary. The plaintiff, who was the beneficiary, brought an action and Sir Robert Megarry V-C found the earlier case conclusive. He held that the plaintiff succeeded, despite the facts that the testator suffered no loss by the misstatement and there was no reliance by the plaintiff. The result seems to have turned on the actual knowledge which the defendant's solicitors had of the plaintiff.

In the light of these two cases, it may be that where a person has actual knowledge that another person may be harmed by a non-defamatory statement made to a third party, then the person making the statement may be liable in negligence if that statement is erroneous. But it sems that actual

---

[18] *Argyll (Duchess of)* v *Argyll (Duke of)* [1965] 1 All ER 615.

[19] *Coco* v *Clark* [1968] FSR 415.

[20] *Furniss* v *Fitchett* [1958] NZLR 396.

[21] *Ministry of Housing and Local Government* v *Sharp* [1970] 1 All ER 1009.

[22] *Ross* v *Caunters* [1979] 3 All ER 580.

physical or economic damage would be a necessary element of any claim. Distress by itself would not suffice.

Similar is the tort of injurious falsehood, in which a false statement made by A to B causes B to act to the detriment of C. This tort overlaps with defamation, but is distinct and may be relevant to invasions of privacy. The plaintiff must prove malice and damage as a consequence. The tort is usually related to commerce, but need not be.

Thus (in contrast with the position in France and Germany, and to some extent in the United Staes) judge-made law in New Zealand affords only an imperfect and incidental safeguard to the privacy of the individual. There are, however, some statutory provisions which have a bearing on privacy, although those protecting privacy are far less numerous than those infringing it.

The Summary Offences Act 1981 provides in s.29 that it is an offence to be "found on property without reasonable excuse". There is no need for the prosecution to prove an intention to commit an offence, but it will be a defence if the defendant satisfies the court that there was no such intention. Section 30 provides that "peeping or peering into a dwelling house" shall be an offence. This includes loitering on land on which a dwelling house is situated, but the offence must take place between one hour after sunset and one hour before sunrise. So the protection offered by both sections is limited.

A piece of legislation of considerable importance to the protection of privacy is the Crimes Amendment Act 1979, which adds a category of Crimes Against Personal Privacy to the principal Act. The key provision is section 216B(1), which lays down that, subject to certain exceptions, every one is liable to a maximum of two years imprisonment who intentionally intercepts any private communication by means of a listening device. "Intercept" is given a broad definition. It "includes hear, listen to, record, monitor or acquire the communication while it is taking place". "Listening device" is defined as "any electronic, mechanical or electromagnetic instrument, apparatus, equipment or other device that is used or is capable of being used to intercept a private communication'. Hearing aids are excepted, as are "devices exempted. . .by Order-in-Council, either generally, or in such places or circumstances or subject to such other conditions as may be specified in that order". This definition is likely to require judicial clarification. Syntactical ambiguity in the first phrase leaves it unclear whether "listening device" is confined to electronic, mechanical or electromagnetic instruments, in which case laser beams may be outside the scope of the Section, or whether the words "other device" are disjunctive and are intended to cover all residual categories of listening devices.

The definition of "private communication" is also likely to require clarification, since it comports standards of reasonableness which may need elaboration.

Section 216B(2)(b) removes liability where the person intercepting the communication does so "pursuant to, and in accordance with the terms of, any authority conferred on him by or under—

i) The Post Office Act 1959; or
ii) The New Zealand Security Intelligence Service Act 1969; or
iii) The Misuse of Drugs Amendment Act 1978".

The authority given by the last two Acts is clear, but the Post Office Act is frustratingly unspecific. Section 158 makes it an offence to interfere with or connect additional apparatus or equipment to the telephone system without the authority of the Postmaster-General. The section implies that he has authority to permit interference with or connexion to the telephone system, but the purposes for which he may exercise this authority are not stated. Since section 158 falls within the part of the Act concerned with Lines and Works, it may be assumed that, in circumstances where interception was necessary for maintenance or installation work, then the authority would be in line with the purposes of the Act. Thus, although the discretion conferred on the Postmaster-General by Section 158 appears to be very wide, it is nevertheless almost certainly confined to the purposes of the Post Office Act,[22a] and it seems that it would be an error to assume that the Postmaster-General has the powers to authorise interceptions for purposes extrinsic to those expressed or implied in the Act. The exception stated in Section 216B(2)(b)(i) of the Crimes Amendment Act is thus concerned only with the powers that the Minister can legitimately exercise for the purposes of the Post Office Act.

Section 216B(3) creates a narrow exception for the police to intercept private communications, other than telephonic communications, by means of a listening device where this is necessary to protect life. Section 216B(1) does apply where telephone conversations are concerned, however, so that the police must have authority extrinsic to the Crimes Amendment Act to intercept a telephone call, even if life is threatened.

Section 216C prohibits the disclosure of private communications unlawfully intercepted except where it is made to a party to the communication or with the consent, express or implied, of a party, as well as in the course of certain investigations and proceedings which are itemised in the section.

Section 216D prohibits dealing with listening devices and provides certain defences: and Section 216E provides for forfeiture of such devices as part of the sentence handed down to an offender by the Court.

The Post Office Act 1959 has a number of sections concerned with privacy. Sections 28 and 29 protect letters (as opposed to other articles) from being opened upon suspicion of an attempt to avoid paying proper postage or containing libellous, seditious, offensive, blasphemous, or gambling matter. Sections 55 to 57 prohibit the unlawful opening of mail in general and Sections 58 and 59 control the divulgence of information obtained from the contents of a postal article. Sections 97, 98, 100 and 101 have similar provisions for telegrams. Section 109 prohibits officers of the Post Office from divulging information from telephone conversations overheard, and Section 110 makes it an offence to use or cause to be used a telephone to disturb, annoy or irritate any person. Section 118, as amended in 1974 protects the secrecy of accounts, bonds and securities and the transactions made by their holders. It should also be noted that while Section 109 prevents officers of the Post Office from divulging phone conversations it does not apply to other people, so anything heard on a party line

[22a] See *Rowling* v *Takaro Properties* [1975] 2 NZLR 65. In *Padfield* v *Minister of Agriculture* [1968] 1 All ER 694, 719 Lord Upjohn pointed out that even an unfettered ministerial discretion is only an unfettered discretion to act lawfully.

would presumably not be protected, and party lines also seem to fall outside the scope of Sections 216A to 216E of the Crimes Amendment Act 1979. Section 158 of the Post Office Act, making it an offence to connect any additional apparatus to the telephone system, has been dealt with above. Interference with the telephone system is also dealt with in the Telephone Regulations 1976/19 regulation 62.

The Inland Revenue Department Act 1974 contains elaborate secrecy provisions and also creates certain classes of privilege between lawyers and between lawyers and their clients for confidential communications provided they relate to legal advice or assistance and do not have the purpose of committing or furthering the commision of some illegal or wrongful act. Certain exceptions apply. Secrecy provisions also apply to Taxation Review Authorities.

The Statistics Act 1975 requires a declaration of secrecy by all employees of the Department. Section 37 provides for security of information: it is to be used only for statistical purposes; only employees making a declaration under Section 21 are to see individual schedules, except for the purpose of a prosecution under the Act; no part of a completed individual schedule and no individual answer is to be communicated or separately published unless such disclosure is consented to in writing by the discloser of the original information; there are certain exceptions, none of which is unduly threatening to privacy. Section 38 makes information acquired privileged and removes the compulsion for any person making a declaration under Section 21 to give oral testimony in proceedings.

The Wanganui Computer Centre Act 1976 expressly proclaims in its long title the intention "to ensure that the system makes no unwarranted intrusion upon the privacy of individuals". Section 5 establishes a Privacy Commissioner who must take an oath of secrecy under Section 10, which is reinforced by Section 12 which extends it to staff. Section 9 sets out the functions and powers of the Privacy Commissioner. These are basically to investigate complaints and to inquire of his own motion into other matters relating to the Act. In particular, Section 9(3) says "Every investigation carried out by the Commissioner shall be conducted in private". Section 14, as amended in 1980, gives individuals the right to apply to the Commissioner for a copy of all or part of the information recorded about him or her on the computer system other than that stored under certain subject headings, which generally fall into the category of current investigations and methods of committing crimes. The Commisisoner must satisfy himself as to the applicant's identity and entitlement to make the application, and he may refuse to release information if, in his opinion, it would be detrimental to the administration of justice. In this he is subject to direction by the Policy Committee. This Committee, set up under Section 19, is charged by Section 22 with determining "the policy of the Computer Centre and the computer system relating to the privacy and the protection of the rights of the individual insofar as these are affected by the operation of the Computer Centre and the computer system. . .". Any person believing information about him or her to be inaccurate may complain to the Commissioner, who must investigate unless he thinks the complaint trivial, frivolous or vexatious, or that an investigation is not necessary having regard to the circumstances of the case (Sections 15 to 18). Section 28

provides for damages for loss or damage caused by incorrect or unauthorised information being made available to any person by the computer system or by any person in the course of operating the computer system, or for authorised information being made available to any person not authorised to receive it. (The Schedule to the Act sets out classes of information and who shall have access to them). Limited damages (up to $500.00) are available for "embarrassment, loss of dignity and injury to the feelings of the plaintiff".

The Public Trust Office Act 1957 Section 17 requires members of the staff, agents and members of the Investment Board to make a declaration of secrecy concerning matters coming to their knowledge in the course of their duties.

The Official Information Act 1982 has had a considerable bearing on privacy. Section 4 states in (b) and (c) that the Act aims to:

(b) provide for proper access by each person to official information relating to that person;

(c) protect official information to the extent consistent with the public interest and the preservation of personal privacy.

Section 9 provides that a "good reason" exists for withholding official information if it is necessary to

(2)(a) protect the privacy of natural persons, including that of deceased natural persons; or

(b) protect information supplied in confidence to any Minister of the Crown or to any Department or organisation; or

(g) maintain the effective conduct of public affairs through —

(ii) the protection of. . .Ministers, officers and employees from improper pressure or harassment; or

(h) maintain legal-professional privilege.

Section 24 gives individuals a right of access to personal information concerning them, and section 25 protects the privacy of this right by providing that the information shall only be released if the individual satisfactorily establishes his or her identity, and that procedures shall be adopted to ensure that any information intended for an individual is received only by that individual in person or by his or her agent.

Section 26 provides for the correction of inaccurate or misleading personal information, and section 27(1)(b) allows refusal to disclose personal information if "the disclosure. . .would involve the unwarranted disclosure of the affairs of another person or of a deceased person". Section 27 also contains certain breach of confidence and other protective provisions.

The full ramifications of the Official Information Act are not yet clear since it only came into force on 1 July 1983, but it may be expected to have a real effect on the law relating to privacy in New Zealand.

The Broadcasting Amendment Act No. 1 1982 has amended the principal Act of 1976 as regards privacy. The 1976 Act requires the Corporation to

have regard to the privacy of the individual when setting programme standards: s.24(1)(g).

The Amendment Act extends the concern for privacy by inserting s.95O into the principal Act. This requires the Broadcasting Complaints Committee under s.95O(1)(b)(ii)

To receive and consider formal complaints of

> Unwarranted infringement of privacy in, or in connection with the obtaining of material included in, programmes broadcast by the Corporation or by a private broadcasting station.

Section 2 of the principal Act is amended so that "a person affected" is redefined:

> In relation to any such unwarranted infringement of privacy as is mentioned in section 95O(1)(b)(ii) of this Act, [a person affected] means a persons whose privacy was infringed.

Section 95Q(1)(c) empowers the Committee not to investigate a complaint under s.95O if it appears that

> . . .the infringement of privacy complained of is a matter in respect of which the person affected has a remedy by way of proceedings in a court of law in New Zealand, and that in the particular circumstances it is not appropriate for the Committee to consider a complaint about it.

Section 95V(1) empowers the Committee to determine the complaint without a formal hearing, but s.95V(2) requires that a complaint concerning infringement of privacy be itself heard in private.

Section 95V(3) requires the complainant to make a declaration in writing that legal action will not be taken in respect of the subject matter of the complaint or the investigation of the complaint by the Committee or the Broadcasting Tribunal.

Under section 95X(1), if the Committee decides that a formal complaint is justified in whole or in part, the Committee

(a) may recommend appropriate action to the broadcasting body by which the programme was broadcast; and

(b) may give to the broadcasting body by which the programme was broadcast directions requiring that body to publish, in any manner specified in the directions, and within such period as may be so specified, a statement which relates to the complaint and which is approved for the purpose by the Committee; and

(c) shall inform the complainant in writing of any action recommended under paragraph (a) of this subsection and of any directions given under paragraph (b) of this subsection.

Section 95X(4) accords to statements broadcast or published under subsection (1)(b) qualified privilege for the purpose of the Defamation Act 1954, First Schedule, Part II, clause 8.

In addition to these specific enactments, there may be occasions when a prosecution for contravention of a Statute under Section 107 of the Crimes Act 1961 could afford some protection of privacy, but the section is vague and problematical, and does not apply if the statutory duty is administrative, ministerial or procedural. It is likely to be of little practical significance as regards privacy. There is also the tort of breach of statutory duty which may be available when an Act creates a duty but lays down on enforcement procedure, but this is also hedged with limitations and will always turn on the intention of the Legislature.

The situation may also arise where a statutory penalty is insufficient to prevent an offender from continuing to commit an offence.[23] In such situations the Attorney-General may take an action seeking to protect the public interest in having the criminal law obeyed. The normal remedy will be an injunction restraining the conduct of the persistent offender, and this may have some value in privacy cases. It should be noted that, an injunction being a civil matter, the burden of proof will be lighter. In many cases the person whose privacy was invaded would have sufficient interest to have locus standi in his or her own right.

By contrast with the few statutory provisions which may, in some circumstances, protect an individual's privacy, there are numerous other statutory provisions which invade it. In his Report for the Year Ended 31 March 1976,[24] the Chief Ombudsman, without claiming to have conducted an exhaustive survey, said he had found at least one hundred and fifty Acts of Parliament empowering governmental officers to enter private property. Four or five more such Acts are added each year. The vast majority of these powers would not be permitted at common law, which basically restricted entry to emergency situations. Most of these statutory powers are concerned with situations where it is deemed socially necessary or desirable that entry should be made. The Chief Ombudsman expressed the opinion that in such cases consent, or at the very least advance notice, should be a necessary prerequisite. In practice, however, few of the existing provisions require, or even provide for, identification of the entrant.

It is proposed here to discuss only two recent Acts which affect adversely the individual's right to privacy, but both of these go considerably further than would normally be considered acceptable in a democratic society.

The first is the New Zealand Security Intelligence Service Act 1969, as amended 1977.[25] Under section 4A of the Act, the Minister may now issue communications interception warrants if he is satisfied that

(a) the interception or seizure of communications is necessary either for detection of activities prejudicial to security or for the purpose of gathering foreign intelligence information essential to security; and

(b) the value of the information justifies interception or seizure; and

---

[23] See, for example *AG* v *Harris* [1960] 3 All ER 207.

[24] Report of the Chief Ombudsman for the Year Ended 31 March 1976, pp. 10-13.

[25] See also a Report by the Chief Ombudsman on the Security Intelligence Service 1976, and the Submissions of the New Zealand Law Society on the Security Intelligence Service Amendment Bill 1977 in [1977] NZLJ 434, as well as the editorial which precedes it.

(c) the information is unlikely to be obtained by other means; and

(d) the information is not privileged in Court proceedings.

It should be noted that "interception" is wider than mere telephone tapping: it could include other listening devices. Further, the warrant authorising interception is not subject to judicial review and there is no machinery for investigating possible abuses. The Act requires a report to Parliament but this is too generalised to afford to a citizen suspecting he or she is under surveillance any means of ascertaining the true position and taking steps to remedy it. There is some residual protection in section 4A(b), which protects people executing an interception warrant by justifying them in taking "any reasonable action necessarily involved". Actions falling outside this limitation are thus potentially examinable by the Courts, but proof of damage would be a real difficulty and there is no provision equivalent to the "embarrassment, loss of dignity, and injury to the feelings" section of the Wanganui Computer Centre Act. Section 48 provides that irrelevant records obtained by interception are to be destroyed and Section 12A prohibits unauthorised disclosure of information. But under Section 12A(1) information which is not related to security but is acquired by means of an interception or seizure can be released with the authorisation of the Minister. This is a dangerous and unnecessary power and is at variance with the policy of the Misuse of Drugs Amendments Act, where such information must be destroyed.

Section 13A contains an ironical reverse protection of anonymity by making it an offence to publish the identity of a member of the Security Intelligence Service or of any person in any way connected with it.

Section 17 provides that a Commissioner of Security Appeals may inquire into complaints by New Zealand residents that their career or livelihood has been adversely affected by any act or omission of the SIS, however Section 22 leaves to the Minister a decision on any action to be taken.

The second Act to be considered is the Misuse of Drugs Amendment Act 1978. Sections 14 to 29 elaborate provisions allowing the police to "intercept a private communication by means of a listening device in any case where there are reasonable grounds for believing that — (a) a person has committed, or is committing, or is about to commit, a drug dealing offence; and (b) it is unlikely that the Police investigation of the case could be brought to a successful conclusion without the grant of such a warrant". The Court of Appeal has recently ruled that the other party to an intercepted telephone conversation can be convicted on the evidence obtained under the warrant although that party was not named in the warrant.

Sections 21 and 22 direct that irrelevant records are to be destroyed and relevant ones are also to be destroyed once it becomes apparent that they will not be required in evidence. Section 23 says that disclosure of private communications lawfully intercepted is prohibited otherwise than in the performance of an officer's duty and Section 25 provides that unlawfully intercepted communications are not admissable in evidence. Most importantly, Section 26 states that lawfully intercepted communications are not admissible where they disclose any offence other than drug dealing. This means that, if in the course of tapping a suspected drug dealer's telephone,

the police hear even a murder confession, they may not use that interception in evidence against the murderer.

Thus it may be seen that, while in New Zealand there are many enactments which reduce people's privacy in a direct manner, some of them to a considerable extent, there is no reciprocal action based squarely on the infringement of privacy as such. There are laws whose operation offers limited protection as a by-product of their principal intent, but this protection is disparate and incomplete. There is no coherent judicial policy regarding the remedies available or appropriate to an individual whose privacy has been invaded.

Attempts have been made in England to introduce general policy legislation but these have failed. The most notable was Lord Mancroft's Right of Privacy Bill in the House of Lords in 1961, which was supported by Lord Goddard and Lord Denning amongst others, but was opposed by the Lord Chancellor, Viscount Kilmuir. During the debate on the Bill both Lord Denning and the Lord Chancellor expressed the opinion that the common law was capable of creating a right of privacy. It may be commented, however, that although this is probably true, it is doubtful whether the Courts could act quickly enough and broadly enough for such action to constitute a real protection for today's citizenry, particularly in view of the speed with which means of invading privacy are multiplying.

Nevertheless, in other jurisdictions the Courts have done so. In the United States, the Courts have created rules far more protective of privacy than any in our law, largely as the result of a famous article written in 1890 by Warren and Brandeis and entitled "The Right to Privacy".[26] The writers relied on early English authorities to demonstrate that the common law "protect[s] those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever their position or station, from having matters which they may properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented".[27] They assert that an action of tort for damages is available in all cases, including compensation for injury to feelings, and that an injunction may also be available in a limited class of cases. They conclude that the common law provides the individual with a weapon against the invasion of his or her privacy "forged in the slow fire of the centuries, and today fitly tempered to his hand".[28]

It may justly be said that modern American privacy law had its origins in this seminal article by Warren and Brandeis, but it has developed considerably since 1891, when judicial notice was first taken of the article. By 1967 the draft Second Restatement of the Laws of Torts identified four separate torts covering the right of privacy: (a) unreasonable intrusion upon the seclusion of another; (b) appropriation of the other's name or likeness; (c) unreasonable publicity given to the other's life; (d) publicity

---

[26] (1890) 4 Harv. LR 193.

[27] Ibid., 214-215.

[28] Ibid., 220.

which unreasonably places the other in a false light before the public.[29] A number of individual States have also legislated to protect privacy. It seems, however, that American law is still inadequate in the areas of lie detection and personality testing, data surveillance, and electronic surveillance where there is no trespass.[30] Nevertheless, the idea of an "inviolate personality", first advanced by Warren and Brandeis, has been extended.[31]

As in the United States, French privacy law is primarily judge-made, although it is broadly based on the general tort provision of the Civil Code,[32] and on press law and Criminal Code provisions[33] The actual content of private life which is protected has not been clearly stated, but a strong distinction is drawn between private persons and people in the public eye, and between private and public life, Thus, although numerous provocative photographs of Brigette Bardot have appeared in the press with her permission, a court was ready to protect her from being photographed in her garden. Even in public, such a person may forbid the publication of a photograph, although in the absence of an express prohibition consent will normally be assumed. Similarly, gossip and anecdotes about a person's private life may not be published without permission, but an historian may portray a contemporary person as long as his facts are properly documented and he is objective.

It may be said as a general proposition that French law protects privacy to a far greater extent than English law.

Under West German law privacy is protected as part of a bundle of rights called the "right of the personality",[34] and this is partly covered by the Federal Constitution of 1949 which protects the "dignity of man" and adds: "Everyone shall have the right to the free development of his personality, in so far as he does not infringe the rights of others or offend against the constitutional order or the moral code".[35]

In an article entitled, "The Right to Privacy in Germany"[36] Krause remarks that, as in France, privacy in Germany is protected by case law. In 1959 a draft code protecting "personality and honour" was drawn up, but it failed to pass into law, largely because its critics reasoned that the judicially-created right had not sufficiently matured to be crystallised in a code. Krause is of the opinion that, in the long run, codification will occur.

In summary, German law at present:

(1) protects the spoken word against unauthorised reception and recording, without the need for publication;

---

[29] See also Prosser (1960) 48 Cal. LR 383.

[30] See Westlin, "Privacy and Freedom".

[31] For an interesting and readable treatment of the development of US privacy law through the cases, see "Privacy: The Right to be Let Alone", by Ernst and Schwartz.

[32] Civil Code Article 1382: "Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer".

[33] See Article 35 of the Press Law of July 19, 1881, as amended on May 6, 1944; and Articles 157, 184 and 378 of the Criminal Code.

[34] Persönlichkeitsrecht.

[35] Federal Constitution (Grundgesetz) Articles 1(1) and 2(1).

[36] "The Right to Privacy in Germany" [1965] Duke LR 481.

(2) prevents the unauthorised taking of photographs;

(3) protects confidential information pertaining to private activities and family life, including letters, diaries and private papers, prohibiting procurement as well as publication;

(4) provides a measure of protection for personal feelings.

Exceptions to the right of privacy include:

(1) where the plaintiff has forfeited his right e.g. by being involved in public affairs;

(2) where the matter complained of is not within the right e.g. by appearin the street, engaging in intimacies on park benches, etc.;

(3) where the defendant's right weighs more heavily than the plaintiff's rendering the defendant's actions privileged;

(4) where public interest is paramount e.g. with constitutionally protected freedoms of speech and the press.

It seems that negligent as well as intentional invasions of the right to personality will be actionable, but subject to the limitation that "the general right of personality does not offer the opportunity of limitless assertion of one's own interests. It is out of the question that claims for damages or rights to injunctions exist wherever someone sees himself hindered by another in his affairs and efforts. . .In each dispute there must be a limitation concerning which the principle of balancing interests must control".[37] There is a solid line of cases assuring the availability of compensation for intangible damage in connexion with injuries to the personality, although it should be noted that most of these involve the unauthorised use of the plaintiff's name or picture in commercial contexts. They could thus be explained as monetary damage involving loss of licence fees for use of name or picture.

Krause sums it up by saying: "There is in Germany today a court-made right to privacy that has been defined quite generously in terms of coverage. It provides an action for negligent as well as intentional invasions and allows damages for all harm including mental distress. . . Privacy has found greater protection in Germany than [U.S. law] has been willing to accord it, but. . .some of this protection has been made available at the expense of other interests which [the American] legal system might be more inclined to favour over privacy interests".[38]

What Krause is implying, which is central to solving the problem of intrusion into people's private lives, is that different societies may choose to strike different balances between the freedom of the individual to be left alone and the freedom of others to find out what they legitimately need to know. In New Zealand, it seems that the balance at present has tipped

[37] Ibid., 507.

[38] Ibid., 516.

against the individual.[39] It might be possible to redress the balance by means of a development of the common law, particularly in the area of torts. But such an approach would be, by its nature, piecemeal. A better solution would appear to be to create a legislated general right of privacy, relating the new to existing legislation and creating not only wider and more direct civil remedies for infringements of privacy, but also criminal sanctions in appropriate cases. The combination of a general statutory tort, reinforced where necessary by criminal sanctions, would offer the individual the most flexible means of retaining his legitimate privacy and of obtaining meaningful remedies for its infringement. A category of exceptions could be created, such as where the public interest outweighs private rights. In such a way legitimate freedoms such as those of the press and of the nation to protect itself against threats to its security could be safeguarded. Statutory defences would also be an important element of any such legislation. Although it might constitute a formidable exercise in drafting, there would be advantages in making a Privacy Act a full codification. As a new area of the law, privacy law would benefit from such treatment, and a code should be able to establish certain presumptions which would induce greater consistency of approach in the future from both legislators and the courts alike. It would be a simple matter for such a code to amend existing legislation to ensure conformity.

It would be desirable in the first instance that a full-scale investigation into privacy be carried out, perhaps by the Chief Ombudsman, or by the Human Rights Commission, which already has jurisdiction to investigate practices and procedures which appear unduly to infringe upon the privacy of the individual and to report to the Prime Minister on the need for reforms.

New Zealand residents do not yet have personal numbers, as, for example, people in Canada do, but our privacy is not less threatened for that. Appropriate action now could again make New Zealand a leader in social legislation in the Commonwealth and enhance generally the quality of life for all who live here.

---

[39] For a good summary in layman's terms of the position, see "The New Zealand Civil Rights Handbook" by Tim McBride, esp. Chapters 10, 11 and parts of Chapter 9.